Certificate

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

D-TRUST GmbH
Kommandantenstraße 15
10969 Berlin, Germany

to confirm that its certification service

D-TRUST Application Certificates CA 3-1 2013

fulfils all requirements defined in the technical specification

ETSI TS 102 042 V2.4.1 (2013-02), policy LCP.

The appendix to the certificate is part of the certificate and consists of 6 pages.

The certificate is valid only in conjunction with the respective evaluation report until 2015-11-30.

ETSI TS 102 042 CA6741.14 TÜVIT® 2014 Trusted Site

Voluntary Validation

Certificate-Registration-No.:
TUVIT-CA6741.14

Essen, 2014-11-28

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

DAkkS Deutsche Akkreditierungsstelle D-ZE-12022-01-01

Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" according to DIN EN 45011 for the scope IT security product certification. The certification body performs its certification on the basis of the following accredited product certification system:

- German document: "Zertifizierungsschema für Zertifikate des akkreditierten Bereichs der Zertifizierungsstelle der TÜV Informationstechnik GmbH", version 1.2 as of 2011-01-28, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report - Surveillance On-Site Inspection - ETSI TS 102 042, D-TRUST Application Certificates CA 3-1 2013", version 1.0 as of 2014-11-25, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 102 042:

- ETSI TS 102 042 V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates", Version 2.4.1, 2013-02, European Telecommunications Standards Institute

The applicable ETSI Certificate Policy is:

- LCP: Lightweight Certificate Policy

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected certification service:

D-TRUST Application Certificates CA 3-1 2013:

Issuer of CA certificate (Root CA or intermediate CA): CN = D-TRUST Root CA 3 2013, Certificate Serial Number: 0f dd ac	
Name of CA (as in certificate)	**serial number of certificate**
CN = D-TRUST Application Certificates CA 3-1 2013	`0f e0 f6`

together with the Certification Practice Statement (CPS) of the operator:

- "Certification Practice Statement der D-TRUST-Root-PKI", version 1.11 as of 2014-11-01, D-TRUST GmbH

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

The ETSI specification ETSI TS 102 042 contains the following requirements:

1 Certification Practice Statement (CPS)

The CA shall have a statement of the practices and procedures.

2 Public key infrastructure – Key management life cycle

The CA shall ensure that CA keys are generated in controlled circumstances.

The CA shall ensure that CA private keys remain confidential and maintain their integrity.

The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties.

If the subject's key is to be used for electronic signatures with the meaning of Directive 1999/93/EC, then the CA shall not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow).

If a copy of the subject's key is kept by the CA then the CA shall ensure that the private key is kept secret and only made available to appropriately authorized persons.

The CA shall ensure that CA private signing keys are not used inappropriately.

The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle.

In case of NCP, the CA shall ensure the security of cryptographic device throughout its lifecycle.

The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured.

In case of NCP+, the CA shall ensure that if it issues to the subject secure user device this is carried out securely.

In case of an EV code signing certificate instructions of appendix H, item 10 of the document “Guidelines for the Issuance and Management of Extended Validation Certificates”, version 1.3, CA/Browser Forum, shall be followed.

3 Public key infrastructure – Certificate Management life cycle

The CA shall ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.

The CA shall ensure that requests for certificates issued to a subject who has previously been registered with the same CA are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes.

The CA shall ensure that it issues certificates securely to maintain their authenticity.

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties.

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties.

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests.

4 CA management and operation

Requirements from document “Network and Certificate System Security Requirements”, CA/Browser Forum, apply.

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

The CA shall ensure that its assets and information receive an appropriate level of protection.

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized.

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure.

The CA shall ensure that CA system access is limited to properly authorized individuals.

The CA shall use trustworthy systems and products that are protected against modification.

The CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible.

The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

The CA shall ensure compliance with legal requirements.

The CA shall ensure that all relevant information concerning a certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

5 Organizational

The CA shall ensure that its organization is reliable.

6 Additional requirements

The CA shall provide different options to allow third parties to check and test their certificates.

In case of PTC-BR, requirements from appendix C of document “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, CA/Browser Forum, apply.

The CA shall disclose all cross certificates that identify the CA as the subject.

In case of PTC-BR, requirements from section 8.4 of document “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, CA/Browser Forum, apply.